UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/787,361	02/27/2004	Hironobu Machida	036741-0130	7946

22428 7590 09/25/2008
FOLEY AND LARDNER LLP
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
RILEY, MARCUS T	
ART UNIT	PAPER NUMBER
2625	
MAIL DATE	DELIVERY MODE
09/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/787,361	**Applicant(s)** MACHIDA ET AL.	
	Examiner MARCUS T. RILEY	**Art Unit** 2625	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) *1, 2, 5, 6, 7, 9 & 11* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,4,7,10 and 12-19* is/are rejected.

7)☒ Claim(s) *14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02/27/04* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *12/18/2007; 02/27/2004* .

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 05, 2008 has been entered.

Response to Amendment

2. This office action is responsive to applicant's remarks received on August 05, 2008. **Claims 3, 4, 7, 10 & 12-19** remain pending and **claims 1, 2, 5, 6, 9 & 11** have been cancelled.

Response to Arguments

3. Applicant's arguments with respect to amended **claims 1, 2, 6, 7-13, 18 & 19** and cancelled **claims 1, 2, 5, 6, 9 &11** filed on August 05, 2008 have been fully considered but they are not persuasive.

A: Applicant's Remarks

Independent Claim 3:

Presently pending independent claim 3 recites a volatile storage means and an image storage means for storing an encryption key, whereby the volatile storage means and the image storage means are provided in a separate unit different from a non-volatile storage means for *storing an encryption key. Thus, even if the unit having the image storage means is stolen, an encryption key itself is prevented from being stolen.*

Kurihara et al. describes that a program for a toner cartridge exchange is encrypted and stored in record medium (such as a CD-ROM), whereby when the program is used, a downloaded encrypted key is used to decrypt the program to be installed in computers.

One difference between the present invention according to claim 3 and Kurihara et al. is that a target of encryption in Kurihara et al. is a control program, whereas a target of encryption in the present invention according to claim 3 is image data for image formation. Clearly, these are much different targets of encryption.

In addition, Kurihara et al. describes a non-volatile environment configuring memory 11. However, Kurihara et al. does not teach or suggest that an encryption key is stored in the non-volatile environment configuring memory 11.

Therefore, even if the volatile storage means described in Bright is applied to Kurihara et al., a non-volatile storage means having an encryption key stored therein would not be obtained from such a combination.

Still further, unlike the present invention according to claim 3, neither Kurihara et al. nor Bright teaches or suggests an image storing means, an encrv-ption an decryption means, and a volatile storage means being provided in a separate unit from a system control unit that contains a non-volatile storage means.

Accordingly, even if Kurihara et al. and Bright are combined, such a Combination would not teach or suggest a structure as explicitly recited in claim 3.

Therefore, presently pending independent claim 3 is patentable over the cited art of record.

<u>Dependent Claims 7 and 10:</u>

Claim 7 recites encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non\- volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means.

Ronning, which is cited against claim 7 along with other prior art, describes data compression and decompression. However, the target of encryption in Ronning is a "sector", and is not an "encryption key" as recited in claim 7.

Accordingly, claim 7, as well as claim 10 that recites similar features, are patentable over the cited art of record.

<u>Independent Claims 12 and 18:</u>

Matsuzaki, which is cited along with other prior art against claims 12 and 18, relates to encrypted communication between a first device and a second device, and Matsuzaki describes a method in which the first device (authorization side) authorizes a validity of the second device (verification side).

Matsuzaki also describes that a random number generated by encryption and a value (random number) generated by decryption are compared. However, unlike the present invention *according to independent claims 12 and 18, Matsuzaki does not compare a plurality of inputted same encryption keys with one another. Note in particular the recitation "key values inputted by a user by a predetermined number of times", as explicitly recited in claims 12 and 18, which is a feature lacking in Matsuzaki.*

With respect to the other cited art of record, Ore describes displaying a list of encrypted files in the form of unencrypted file names (see column 6, lines 9-12 of Ote). Kobayashi et al. describes that image memory sizes are divided to transmit a part when an unoccupied capacity for an image memory is secured (see column 18, lines 41-47 of Kobayashi et al.). Ashizaki describes performing either a decimal format or a hexadecimal format (see column 15, lines 4-6 of Ashizaki). None of these secondary references rectifies the above-mentioned deficiencies of Matsuzaki.

Accordingly, independent claims 12 and 18 patentably distinguish over the cited art of record.

A: Examiner's Response

Independent Claim 3:

Independent claim 3 recites a volatile storage means and an image storage means for storing an encryption key, whereby the volatile storage means and the image storage means are provided in a separate unit different from a non-volatile storage means for storing an encryption key.

Bright '329 discloses wherein the non-volatile storage means is provided in a system control unit for controlling image forming processing and wherein the image storing means, the volatile storage means, and the encryption and decryption means are arranged in a separate unit from the system control unit (See Figure 2 and *"The CPU 38 performs most of the work of the Hard-Node. It does the encryption and decryption, authorization checks, communications with the host machine 32, and directs the activities of the data channels 54. The CPU 38 operates under control of a program, stored in Program Storage 56. This is one of the several sections of storage addressable by the CPU, the others being Scratchpad Storage 58 and the Superkey Register 60. Scratchpad Storage 58 is used for buffers, intermediate encryption results and other temporary data. The Superkey Register holds the Hard-Node's own Superkey under which the Key Data Base, at least, is encrypted. For maximum security, it is recommended that the Superkey Register 60 be a volatile storage device with its own battery and interlock to remove all power in case the enclosure 42 is tampered with or opened. The Scratchpad Storage 58 should be a volatile random access memory device, while the Program Storage 56 should be a nonvolatile ROM (read only memory) device."* column 3, lines 12-31). Moreover, Bright '329 discloses that the CPU 38 does the encryption and decryption separately from the volatile storage 60, the nonvolatile storage 56. Figure 2 show that each of these items is a separate unit from the control system.

Kurihara et al. does teach or suggest that an encryption key is stored in the non-volatile environment configuring memory 11 (*"An environment configuring memory 11 comprising a non-volatile read/write memory (referred to as an "NVRAM" below) saves various operating environment settings of the image forming apparatus 30.* column 2, lines 27-30). See also (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who* *meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

Accordingly, presently pending independent claim 3 is not patentable over the cited art of record.

Dependent Claims 7 and 10:

Claim 7 recites encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non\- volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means. (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25). See also (*"An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18).

In addition, Ronning discloses in FIG. 16B a flow chart of a preferred varying positional key encryption/decryption routine used with the routine of FIG. 16A. Although, Ronning does disclose sector encryption/decryption, Ronning also discloses key encryption/decryption in FIG. 16B. Here, The routine in FIG. 16B performs the actual encryption/decryption of data and is an example of how to encrypt/decrypt the encrypted packages 62 and 68 (see FIG. 4A) which contain the distributed software programs or digital information and usage files. Other encryption schemes are possible. The significance of the encryption scheme is in providing protection of the distributed information so that one may not obtain an unauthorized copy of the information without considerable time, effort, and processing capability.

Accordingly, claim 7, as well as claim 10 that recites similar features, are not patentable over the cited art of record.

Independent Claims 12 and 18:

Matsuzaki does compare a plurality of inputted same encryption keys with one another.

Matsuzaki '476 discloses key value determining means for determining whether key values input by the user by a predetermined number of times match each other (*"First device 11 compares the decryption result RR1 with the random number R1 temporarily stored inside first device 11. If they match, first device 11 considers second device 12 to be in possession of the same authentication key S, and confirms the entity in communication as a legitimate device. However if they do not match, then it judges the entity in communication an unauthorized device and terminates the process."* column 2, lines 49-56).

Ronning '647 discloses a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other (*"The system then determines if the loaded image matches the database image (196) for security purposes. If the image does not match, the database data is rectified to that of the image (198) and the virtual volume is closed and unmounted (194) in order to maintain the application in a locked state."* column 9, lines 5-9). See also (*"An image file 77 which is the desired size of a* *"virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18);

Accordingly, independent claims 12 and 18 are not patentably distinguishable over the cited art of record.

Thus, Applicant's arguments with respect to amended **claims 1, 2, 6, 7-13, 18 & 19** and cancelled **claims 1, 2, 5, 6, 7, 9 &11** filed on August 05, 2008 have been fully considered but they are not persuasive. As a result, the present application is not in condition for allowance.

Claim Objections

(The previous claim objections are withdrawn in light of the applicant's amendments.)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claim 3** is rejected under 35 U.S.C. 103(a) as being unpatentable Kurihara (US 6,850,716 B2 hereinafter, Kurihara '716) in combination with Bright et al. (US 4,262,329 hereinafter, Bright '329).

Regarding claim 3; Kurihara '716 discloses an image forming apparatus for forming an image based on input image data, the image forming apparatus comprising (*"The dot-pattern data from the dot-pattern memory 10 is input to the FIFO (First In, First Out) memory 7, which* *outputs this data to an interface 8 for an image forming unit 20."* column 2, lines 1-4): an image storing means for storing the input image data (*"The dot-pattern memory 10 is a memory for storing data-pattern data that has been expanded into a pattern by the processing program stored in the program ROM 6 in order to form the dot pattern."* column 1, lines 64-67); non-volatile storage means for storing an encryption key (*"An environment configuring memory 11 comprising a non-volatile read/write memory (referred to as an "NVRAM" below) saves various operating environment settings of the image forming apparatus 30.* column 2, lines 27-30). See also (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39); encryption and decryption means that encrypts image data using the encryption key prior to the storage of the input image data onto the image storage means, and decrypts the encrypted image data subsequent to the reading of the encrypted image data from the image storage means (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

Kurihara '716 does not expressly disclose a volatile storage means that reads and stores the encryption key stored in the non-volatile storage means when power is on; wherein the non-volatile storage means is provided in a system control unit for controlling image forming processing and wherein the image storing means, the volatile storage means, and the encryption and decryption means are arranged in a separate unit from the system control unit.

Bright '329 discloses a volatile storage means that reads and stores the encryption key stored in the non-volatile storage means when power is on (*"The CPU 38 performs most of the work of the Hard-Node. It does the encryption and decryption, authorization checks, communications with the host machine 32, and directs the activities of the data channels 54. The CPU 38 operates under control of a program, stored in Program Storage 56. This is one of the several sections of storage addressable by the CPU, the others being Scratchpad Storage 58 and the Superkey Register 60. Scratchpad Storage 58 is used for buffers, intermediate encryption results and other temporary data. The Superkey Register holds the Hard-Node's own Superkey under which the Key Data Base, at least, is encrypted. For maximum security, it is recommended that the Superkey Register 60 be a volatile storage device with its own battery and interlock to remove all power in case the enclosure 42 is tampered with or opened. The Scratchpad Storage 58 should be a volatile random access memory device, while the Program Storage 56 should be a nonvolatile ROM (read only memory) device."* column 3, lines 12-31); See also (*"At log-on time, it sends an encrypted password to identify the user to the central site Hard-Node, which looks it up in its Key Data Base. The user's key is entered into the micro-Hard-Node's volatile Key Register (analogous to the Hard-Node's Superkey Register) via a Key Entry device, which may be a magnetic stripe reader."* column 5, lines 19-26); wherein the non-volatile storage means is provided in a system control unit for controlling image forming processing and wherein the image storing means, the volatile storage means, and the encryption and decryption means are arranged in a separate unit from the system control unit (See Figure 2 and *"The CPU 38 performs most of the work of the Hard-Node. It does the encryption and decryption, authorization checks, communications with the host machine 32, and directs the activities of the data channels 54. The CPU 38 operates under control of a program, stored in Program Storage 56. This is one of the several sections of storage addressable by the CPU, the others being Scratchpad Storage 58 and the Superkey Register 60. Scratchpad Storage 58 is used for buffers, intermediate encryption results and other temporary data. The Superkey Register holds the Hard-Node's own Superkey under which the Key Data Base, at least, is encrypted. For maximum security, it is recommended that the Superkey Register 60 be a volatile storage device with its own battery and interlock to remove all power in case the enclosure 42 is tampered with or opened. The Scratchpad Storage 58 should be a volatile random access memory device, while the Program Storage 56 should be a nonvolatile ROM (read only memory) device."* column 3, lines 12-31).

Kurihara '716 and Bright '329 are combinable because they are from same field of endeavor of data processing systems (*"It is an object of this invention to provide a new and improved data processing security system."* Bright '329 at column 3, lines 15-16).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the data processing system as taught by Kurihara '716 by adding a volatile storage means that reads and stores the encryption key stored in the non-volatile storage means when power is on; wherein the non-volatile storage means is provided in a system control unit for controlling image forming processing and wherein the image storing means, the volatile storage means, and the encryption and decryption means are arranged in a separate unit from the system control unit as taught by Bright '329.

The motivation for doing so would have been because it is advantageous to provide to provide a new and improved security system for data processing installations which is especially suitable for commercial use (*"Another object is to provide a new and improved security system for data processing installations which is especially suitable for commercial use."* Bright '329 at column 1, lines 47-49).

Therefore, it would have been obvious to combine Kurihara '716 with Bright '329 to obtain the invention as specified in claim 1.

6. **Claims 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716 in combination with Bright '329 as applied to claim 3 above, and further in view of Lee et al. (US 5,606,613 hereinafter, Lee '613).

Regarding claim 4; Kurihara '716 and Bright '329 as modified does not expressly disclose an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number.

Lee '613 discloses an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number (*"In operation, upon power-up of the system or at such other selected times, the verification circuit in response to a power-up print command (Print Cmmd) from the meter 10 outputs a random number message to the decryption/encryption engine 37 which encrypts the message in response to the power-up print command. The encrypted message is sent out to the meter. The* *encryption/decryption engine 37 of the vault decrypts the message in response to the print command."* column 3, lines 61-67 thru column 4, lines 1-2).

Kurihara '716 and Bright '329 are combinable with Lee '613 because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a postage metering system using digital printing…"* Lee '613 at column 1, lines 6-7).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716 and Bright '329 by adding an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number as taught by Lee '613.

The motivation for doing so would have been in order to assure full and accurate accounting of the printer (*" In order to assure full and accurate accounting for the particular digital printer, upon power-up of the system or at such other pre-selected condition, the print controller module of the digital printer sends out an encrypted message to the meter."* Lee '613 at column 2, lines 14-19).

Therefore, it would have been obvious to combine Kurihara '716 and Bright '329 with Lee '613 to obtain the invention as specified in claim 3.

7. **Claims 7 & 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716, Bright '329 and Lee '613 as applied to claim 3 above, and further in view of Ronning '647.

Regarding claim 7; Kurihara '716, Bright '329 and Lee '613 as modified does not expressly disclose an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means.

Ronning '647 discloses an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25). See also (*"An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18).

Kurihara '716, Bright '329 and Lee '613 are combinable with Ronning '647 because they are from same field of endeavor of an image forming apparatus (*"The system typically uses an image driver 56..."* Ronning '647 at column 5, lines 19-20).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716, Bright '329 and Lee '613 by adding an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means as taught by Ronning '647.

The motivation for doing so would have been in order to prevent unauthorized copying of the software program or other digital information (*"...in order to prevent unauthorized copying of the software program or other digital information."* Ronning '647 at column 2, lines 20-23).

Therefore, it would have been obvious to combine Kurihara '716, Bright '329 and Lee '613 with Ronning '647 to obtain the invention as specified in claim 3.

Regarding claim 10; Ronning '647 discloses where the encryption key compression and decompression means applies an image compression and decompression unit for compressing or decompressing the image data (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25).

8. **Claims 12 & 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Kurihara '716, Matsuzaki et al. (US 6,058,476 hereinafter, Matsuzaki '476) and Ronning '647 as applied to claim 12 above, and further in view of Ote '506.

Regarding claim 12; Kurihara '716 discloses an image forming apparatus for forming an image based on input image data, the image forming apparatus comprising (*"The dot-pattern data from the dot-pattern memory 10 is input to the FIFO (First In, First Out) memory 7, which outputs this data to an interface 8 for an image forming unit 20."* column 2, lines 1-4): an image storing means for storing the input image data (*"The dot-pattern memory 10 is a memory for storing data-pattern data that has been expanded into a pattern by the processing program stored in the program ROM 6 in order to form the dot pattern."* column 1, lines 64-67).

Kurihara '716 does not expressly disclose input means for capturing a key value of an encryption key input by a user during the setting of the encryption key; key value determining means for determining whether key values input by the user by a predetermined number of times match each other.

Matsuzaki '476 discloses input means for capturing a key value of an encryption key input by a user during the setting of the encryption key (*"In FIG. 3 step (11), the E function 67 uses data transfer key K stored in data transfer key K storage unit 70 to encrypt digital copyrighted material inputted through external I/F unit 61 and switch 65. The result Cj is outputted to second device 52 through switch 68 and external I/F unit 61."* column 15, lines 3-7); key value determining means for determining whether key values input by the user by a predetermined number of times match each other (*"First device 11 compares the decryption result RR1 with the random number R1 temporarily stored inside first device 11. If they match, first device 11 considers second device 12 to be in possession of the same authentication key S, and confirms the entity in communication as a legitimate device. However if they do not match,* *then it judges the entity in communication an unauthorized device and terminates the process."* column 2, lines 49-56).

Kurihara '716 and Matsuzaki '476 are combinable because they are from same field of endeavor of an image forming apparatus (*"FIG. 12 is a block diagram showing the configuration of the image playback apparatus 111 shown in FIG. 9."* Matsuzaki '476 at column 11, lines 1-2). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716 by adding input means for capturing a key value of an encryption key input by a user during the setting of the encryption key; key value determining means for determining whether key values input by the user by a predetermined number of times match each other as taught by Matsuzaki '476.

The motivation for doing so would have been to provide an encryption device possessing the minimum functions necessary for ensuring the security of communication between devices using only a small encryption IC (*"The primary object of the present invention is to provide an encryption device possessing the minimum functions necessary for ensuring the security of communication between devices using only a small encryption IC."* Matsuzaki '476 at column 5, lines 29-32).

Therefore, it would have been obvious to combine Kurihara '716 and Matsuzaki '476 to obtain the invention as specified in claim 12.

Kurihara '716 and Matsuzaki '476 as modified does not expressly disclose a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other; encryption and decryption means for encrypting the image data using an encryption key prior to the storage of the input image data onto image storage means, and for decrypting the encrypted image data subsequent to the reading of the encrypted image data from the image storage means.

Ronning '647 discloses a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other (*"The system then determines if the loaded image matches the database image (196) for security purposes. If the image does not match, the database data is rectified to that of the image (198) and the virtual volume is closed and unmounted (194) in order to maintain the application in a locked state."* column 9, lines 5-9). See also (*"An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18); and encryption and decryption means for encrypting the image data using an encryption key prior to the storage of the input image data onto image storage means, and for decrypting the encrypted image data subsequent to the reading of the encrypted image data from the image storage means (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25).

Kurihara '716 and Matsuzaki '476 are combinable with Ronning '647 because they are from same field of endeavor of an image forming apparatus (*"The system typically uses an image driver 56..."* Ronning '647 at column 5, lines 19-20).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716 and Matsuzaki '476 by adding a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other or encryption and decryption means for encrypting the image data using an encryption key prior to the storage of the input image data onto image storage means, and for decrypting the encrypted image data subsequent to the reading of the encrypted image data from the image storage means as taught by Ronning '647.

The motivation for doing so would have been in order to prevent unauthorized copying of the software program or other digital information (*"...in order to prevent unauthorized copying of the software program or other digital information."* Ronning '647 at column 2, lines 20-23).

Therefore, it would have been obvious to combine Kurihara '716 and Matsuzaki '476 with Ronning '647 to obtain the invention as specified in claim 12.

Kurihara '716, Matsuzaki '476 and Ronning '647 does not expressly disclose displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on.

Ote '506 discloses displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on (*"Upon starting the file encryption/decryption means 1000 to conduct decryption, the file encryption/decryption means 1000 conducts authentication processing by using the password 1070 with respect to a user input password, then refers to the unencrypted file /encrypted file association table 1060, and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file names. In this state, the encryption folder 1040 is open. The user can select unencrypted files 1090 stored in the encrypted file area 1080 out of the list displayed in the form of uncrypted file names."* column 5, lines 5-15).

Kurihara '716, Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus (*"The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen."* Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Kurihara '716, Matsuzaki '476 and Ronning '647 by adding displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Kurihara '716, Matsuzaki '476 and Ronning '647 with Ote '506 to obtain the invention as specified in claim 12.

Regarding claim 13; The combination Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 as modified does not expressly disclose display means for displaying the key value captured by the input means, and converting an input key value into a form having no specific meaning.

Ote '506 discloses display means for displaying the key value captured by the input means, and converting an input key value into a form having no specific meaning (*"...and* *displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file name."* column 6, lines 9-12).

Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus (*"The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen."* Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 by adding display means for displaying the key value captured by the input means, and converting an input key value into a form having no specific meaning as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 with Ote '506 to obtain the invention as specified in claim 12.

8. **Claims 18 & 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Matsuzaki '476 and Ronning '647 as applied to claim 18 above, and further in view of Ote '506.

Regarding claim 18; Matsuzaki '476 discloses a method for inputting the setting of an encryption key for use in the encryption of image data, the encryption key being used to store input image data in image storage means, the method comprising the steps of: capturing key values of the encryption key input by a user (*"In FIG. 3 step (11), the E function 67 uses data transfer key K stored in data transfer key K storage unit 70 to encrypt digital copyrighted material inputted through external I/F unit 61 and switch 65. The result Cj is outputted to second device 52 through switch 68 and external I/F unit 61."* column 15, lines 3-7); determining whether the key values input by the user by a predetermined number of times match each other (*"First device 11 compares the decryption result RR1 with the random number R1 temporarily stored inside first device 11. If they match, first device 11 considers second device 12 to be in possession of the same authentication key S, and confirms the entity in communication as a legitimate device. However if they do not match, then it judges the entity in communication an unauthorized device and terminates the process."* column 2, lines 49-56).

Matsuzaki '476 does not expressly disclose storing, in non-volatile storage means, the input key value as the encryption key when the key values match each other in the key value determining step.

Ronning '647 discloses storing, in non-volatile storage means, the input key value as the encryption key when the key values match each other in the key value determining step (*"The system then determines if the loaded image matches the database image (196) for security purposes. If the image does not match, the database data is rectified to that of the image (198) and the virtual volume is closed and unmounted (194) in order to maintain the application in a locked state."* column 9, lines 5-9). See also (*"An image file 77 which is the desired size of a* *"virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18).

Matsuzaki '476 and Ronning '647 are combinable because they are from same field of endeavor of an image forming apparatus (*"The system typically uses an image driver 56..."* Ronning '647 at column 5, lines 19-20).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476 by adding storing, in non-volatile storage means, the input key value as the encryption key when the key values match each other in the key value determining step as taught by Ronning '647.

The motivation for doing so would have been in order to prevent unauthorized copying of the software program or other digital information (*"...in order to prevent unauthorized copying of the software program or other digital information."* Ronning '647 at column 2, lines 20-23).

Therefore, it would have been obvious to combine Matsuzaki '476 with Ronning '647 to obtain the invention as specified in claim 18.

Matsuzaki '476 and Ronning '647 does not expressly disclose displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on.

Ote '506 discloses displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on (*"Upon starting the file encryption/decryption means 1000 to conduct decryption, the file encryption/decryption means 1000 conducts authentication processing by using the password 1070 with respect to a user input password, then refers to the unencrypted file /encrypted file association table 1060, and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file names. In this state, the* *encryption folder 1040 is open. The user can select unencrypted files 1090 stored in the encrypted file area 1080 out of the list displayed in the form of uncrypted file names."* column 5, lines 5-15).

Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus (*"The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen."* Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Matsuzaki '476 and Ronning '647 by adding displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Matsuzaki '476 and Ronning '647 with Ote '506 to obtain the invention as specified in claim 18.

Regarding claim 19; Matsuzaki '476 in combination with Ronning '647 does not expressly disclose wherein the displaying step displays the key value captured in the capturing step, and converts an already input key value into a form having no specific meaning.

Ote '506 discloses wherein the displaying step displays the key value captured in the capturing step, and converts an already input key value into a form having no specific meaning (*"...and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file name."* column 6, lines 9-12).

Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus (*"The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen."* Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Matsuzaki '476 and Ronning '647 by adding a wherein the displaying step displays the key value captured in the capturing step, and converts an already input key value into a form having no specific meaning as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Matsuzaki '476 and Ronning '647 with Ote '506 to obtain the invention as specified in claim 18.

10. **Claims 15, 16 & 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 as applied to claim 12 above, and further in view of Ashizaki '500.

Regarding claim 15; Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 does not expressly disclose where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format.

Ashizaki '500 discloses where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format (*"As shown in FIGS. 9 to 12, the print data specifying information is identified by a hexadecimal value of the name of an image format."* column 15, lines 4-6).

Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 are combinable with Ashizaki '500 because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a... printing apparatus..."* Ashizaki '500 at column 1, lines 12-13).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716, Matsuzaki '476, Ronning '647 and Ote '506 by adding where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format as taught by Ashizaki '500.

The motivation for doing so would have been in order to make a printing work by the use of the print data supplied from the printing control unit via the second input/output means (*"...for making a printing work by the use of the print data supplied from the printing control unit via the second input/output means."* Ashizaki '500 at column 5, line 1-2).

Therefore, it would have been obvious to combine Kurihara ‘716, Matsuzaki ‘476, Ronning ‘647 and Ote ‘506 with Ashizaki ‘500 to obtain the invention as specified in claim 12.

Regarding claim 16; Ashizaki ‘500 discloses where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format (*“As shown in FIGS. 9 to 12, the print data specifying information is identified by a hexadecimal value of the name of an image format.”* column 15, lines 4-6).

Regarding claim 17; Ashizaki ‘500 discloses where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format (*“As shown in FIGS. 9 to 12, the print data specifying information is identified by a hexadecimal value of the name of an image format.”* column 15, lines 4-6).

Allowable Subject Matter

8. **Claim14** is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Marcus T. Riley whose telephone number is 571-270-1581. The examiner can normally be reached on Monday - Friday, 7:30-5:00, est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Twyler Lamb can be reached on 571-272-7406. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Marcus T. Riley
Assistant Examiner
Art Unit 2625

/Marcus T Riley/
Examiner, Art Unit 2625

/Twyler L. Haskins/
Supervisory Patent Examiner, Art Unit 2625